Please REPLACE the paragraph beginning at page 42, line 31, as follows:

In FIGURES 33A, 33B, 34A and 34B, the input mask FMin may be eliminated similarly to the Rijndael method described above. However, FMout can not be eliminated in the same manner as the Rijndael method. FIGURE 35 shows the propagation of the influence of the mask over plural rounds of the Feistel encryption device. In FIGURE 35, a solid line indicates a masked path. The FMout can not be eliminated, because, in the Feistel encryption, the data (A) masked in a certain round affects not only the next round (B) but also the subsequent rounds (C) as shown in FIGURE 35.

IN THE CLAIMS:

Please REPLACE the following claims:

12. (AS ONCE AMENDED HEREIN) The encryption device according to claim 10, wherein

each of said nonlinear transform means nonlinearly transforms an input thereto in accordance with a fixed table.

REMARKS

The foregoing specification amendments correct citations therein of various designations of the figures to include designations "A" and "B" so as to be consistent with the actual figure legends.

The foregoing amendment to claim 12 corrects a typographical error, thereby to present a singular subject consistent with the singular verb "transforms."

No new matter is presented.

Approval and entry of the foregoing specification and claim amendments are respectfully requested.

If there are any additional fees associated with filing of this Amendment, please charge the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: January 30, 2002

By: ______________________
H. J. Staas
Registration No. 22,010

700 Eleventh Street, NW, Suite 500
Washington, D.C. 20001
(202) 434-1500

VERSION WITH MARKINGS TO SHOW CHANGES MADE

IN THE SPECIFICATION:

Please AMEND the paragraph beginning at page 8, line 30, as follows:

When the conventional encrypting process in which the conventional key XOR function, the linear function, and the nonlinear function as shown in FIGURES 2, 3 and 4 are used is changed to the encrypting process shown in FIGURE 10, they are replaced with a key XOR function, a linear function, and a nonlinear function as shown in FIGURES 11, 12 and [13] 13A, respectively, in accordance with the random mask value method.

Please AMEND the paragraph beginning at page 9, line 1, as follows:

In the random mask value method, the computation of the conventional intermediate data X_i in the encryption is replaced with the computation of the X_i' and the random number R_i which satisfy the exclusive OR, $X_i = X_i'$ XOR R_i. The encrypting unit computes X_i', and the mask value generating unit computes R_i. The following equations (7) are established for X_i, X_i', Z_i, Z_i', R_i, and RO_i in the operations shown in FIGURES 2 and 11, FIGURES 3 and 12, and FIGURES 4 and [13] 13A.

Please AMEND the paragraph beginning at page 40, line 9, as follows:

FIGURE 33A shows an example of the first type of encryption device 100 shown in FIGURE 21, which is an encryption device 700 in accordance with the DES encryption of [FIGURE 32] FIGURES 32A and 32B to which the fixed mask value method is applied in a manner similar to the encryption device 400 of FIGURE 29. FIGURE 33B shows a more detailed configuration of a F function shown in FIGURE 33A. In FIGURE 33A, the processor 150, the memories 160, 162 and 164 shown in FIGURE 21 are not shown for simplicity.

Please AMEND the paragraph beginning at page 41, line 15, as follows:

The processor 150 in FIGURE 21 controls the processing elements 701 to 763 and the like of the encryption device 700 of [FIGURE 33] FIGURES 33A and 33B in accordance with the program stored in the program memory 160. Alternatively, the processor 150 may provide the processing elements 701 to 763 and the like, by executing the program in the memory 160 which is implemented to provide the functions corresponding to the processing elements 701 to 763 and the like. In this case, [FIGURE 33] FIGURES 33A and 33B may be considered as a flow diagram.

Please AMEND the paragraph beginning at page 41, line 26, as follows:

FIGURE 34A shows an example of the second type of encryption device 200 shown in FIGURE 24, which is an encryption device 800 in accordance with the DES encryption of [FIGURE 32] FIGURES 32A and 32B to which the fixed mask value method is applied in a manner similar to the encryption device 500 of FIGURE 31. FIGURE 34B shows a more detailed configuration of a F function shown in FIGURE 34A. In FIGURE 34A, the processor 250, the memory 260, 262 and 264 shown in FIGURE 24 are not shown for simplicity.

Please AMEND the paragraph beginning at page 42, line 5, as follows:

The processor 250 in FIGURE 24 controls the processing elements 801 to 862 and the like of the encryption device 800 of [FIGURE 34] FIGURES 34A and 34B in accordance with the program stored in the memory 260. Alternatively, the processor 150 may provide the processing elements 801 to 862 and the like, by executing the program in the memory 160 which is implemented to provide the functions corresponding to the processing elements 801 to 862 and the like. In this case, [FIGURE 34] FIGURES 34A and 34B may be considered as a flow diagram.

Please AMEND the paragraph beginning at page 42, line 31, as follows:

In FIGURES [33 and 34] 33A, 33B, 34A and 34B, the input mask FMin may be eliminated similarly to the Rijndael method described above. However, FMout can not be eliminated in the same manner as the Rijndael method. FIGURE 35 shows the propagation of the influence of the mask over plural rounds of the Feistel encryption device. In FIGURE 35, a solid line indicates a masked path. The FMout can not be eliminated, because, in the Feistel encryption, the data (A) masked in a certain round affects not only the next round (B) but also the subsequent rounds (C) as shown in FIGURE 35.

IN THE CLAIMS:

Please AMEND the following claims:

12. (ONCE AMENDED) The encryption device according to claim 10, wherein each of said nonlinear transform means nonlinearly transforms an input thereto in accordance with a fixed table.